

| <b>Recipe 16 - Configuration Guide for Setting up Trustgenix IdentityBridge 2.1 as an AA and CS</b> |  |
|---|--|
| <b>Table of Contents:</b>   |  |
| 1   | Setup..... 1                             |
| 1.1   | Terms and Introduction ..... 1           |
| 2   | Partner Configuration ..... 2            |
| 2.1   | Open Trustgenix for Configuration..... 2 |
| 2.2   | Configure a Partner AA..... 4            |
| 2.3   | Configure a Partner CS ..... 11          |
| <b>Version 2.0.0</b>  |  |

## 1 Setup

### 1.1 Terms and Introduction

The SAML 1.0 is one of the adopted schemes within the E-Authentication architectural framework. This guide should help you setup SAML 1.0 and Trustgenix IdentityBridge 2.1 as an Agency Application (AA) and Credential Service (CS). Remember that the Trustgenix setup screens are often the same, whether setting up an AA or a CS. After reviewing the terms, configure your scheme to handle SAML 1.0, starting at the administration console screen shown in Figure 16-1.

| Term                              | Definition   |
|-----------------------------------|--|
| Agency Application (AA)           | An online service provided by a government agency that requires an end user to be authenticated.   |
| Credential Service (CS)           | A service of a CSP that provides credentials to subscribers for use in electronic transactions. If a CSP offers more than one type of credential, then each one is considered a separate CS. |
| Credential Service Provider (CSP) | An organization that offers one or more CSs. Sometimes known as an Electronic Credential Provider (ECP).   |
| Project Management Office (PMO)   | The PMO is the organization that handles E-Authentication program management, administration, and operations.  |

## 2 Partner Configuration

### 2.1 Open Trustgenix for Configuration

Open the Trustgenix IdentityBridge Administration Console (<https://<host>/tfs-internal/admin>). The administration console screen should appear as shown in Figure 16-1 (*note: the product names provided may be different*). Next, click on the **New Site** link provided in the left-hand Admin Tasks column.

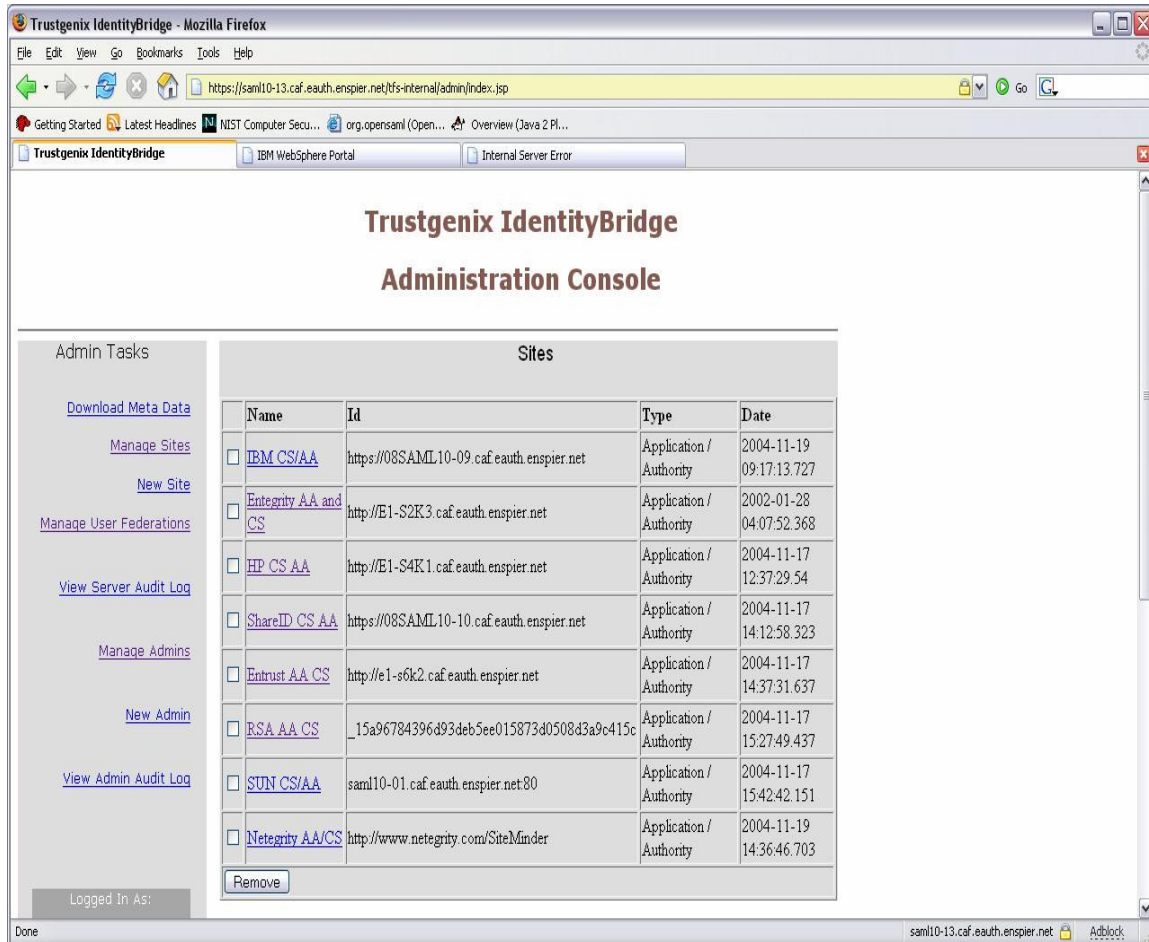


Figure 16-1: Administration Console

The New Site screen should appear as shown in Figure 16-2.

The screenshot shows a web browser window titled "Trustgenix IdentityBridge - Microsoft Internet Explorer". The address bar displays "https://sam10-13.caf.enspiner.net/tfs-internal/admin/newsite.jsp". The browser's toolbar includes buttons for Back, Forward, Search, Favorites, Media, and a search engine dropdown set to Google. The main content area is titled "Trustgenix IdentityBridge Administration Console". On the left, a sidebar labeled "Admin Tasks" contains links: "Download Meta Data", "Manage Sites", "New Site", "Manage User Federations", "View Server Audit Log", "Manage Admins", "New Admin", and "View Admin Audit Log". At the bottom of the sidebar, it says "Logged In As:". The main content area features a "New Site" form with the following fields: "Site Type" (a dropdown menu showing "Application (SP)"), "Site Name", "Homepage URL", "Description", "Logo URL", "Logo Text", and "Protocol" (a dropdown menu showing "Liberty 1.2"). A "Next" button is located at the bottom of the form.

**Figure 16-2: New Site Screen**

## 2.2 Configure a Partner AA

As demonstrated in Figure 16-3 below, select **Application** from the **Site Type** drop down menu, enter a **name** for the site in the **Site Name** field, enter a **target URL** for the site in the **Homepage URL** field, enter a **description** of the site in the **Description** field (*optional*), select **SAML 1.0** from the **Protocol** drop down menu, and then click the **Next** button.

The screenshot shows a web browser window titled "https://saml10-13.caf.eauth.enspier.net/tfs-internal/admin/newsite.jsp - Microsoft Internet Explorer". The browser's address bar shows the URL. The page content is titled "Trustgenix IdentityBridge Administration Console". On the left, there is a sidebar with "Admin Tasks" including links for "Download Meta Data", "Manage Sites", "New Site", "Manage User Federations", "View Server Audit Log", "Manage Admins", "New Admin", and "View Admin Audit Log". The main content area is titled "New Site" and contains a form with the following fields: "Site Type" (a dropdown menu with "Application (SP)" selected), "Site Name" (a text field with "Sample Site Name"), "Homepage URL" (a text field with "http://www.samplesite.co"), "Description" (a text field with "Description of App"), "Logo URL" (an empty text field), "Logo Text" (an empty text field), and "Protocol" (a dropdown menu with "SAML 1.0" selected). A "Next" button is located at the bottom of the form. At the bottom left of the page, it says "Logged In As:".

**Figure 16-3: Select Application**

The New Site Meta Data screen should appear as shown in Figure 16-4. As demonstrated in Figure 16-4, select the **Manual Entry** radio button, enter a **unique Audience ID** for the site (e.g. <https://<host>>) in the **Audience ID** field, past the **base64 encoded client certificate** of the partner in the **Assertion Consumer Certificate** field (*note: delete the “being certificate” and “end certificate” header and footer if provided*), enter the **Artifact receiver URL** in the **Assertion Consumer URL** field, and then click the **Create** button.

The screenshot shows a web browser window titled "Trustgenix IdentityBridge - Microsoft Internet Explorer". The address bar shows the URL "https://sam10-13.caf.ensper.net/tfs-internal/admin/upload.jsp". The page title is "Trustgenix IdentityBridge Administration Console".

On the left side, there is a sidebar with the following links: "Admin Tasks", "Download Meta Data", "Manage Sites", "New Site", "Manage User Federations", "View Server Audit Log", "Manage Admins", "New Admin", and "View Admin Audit Log". At the bottom of the sidebar, it says "Logged In As:".

The main content area is titled "New Site Meta Data". It contains the following fields and controls:

- Type Application**: A label above the "Protocol" field.
- Protocol**: A text field containing "SAML 1.0".
- Meta Data File**: A text field with a "Browse..." button next to it.
- Meta Data URL**: A text field.
- Manual Entry**: A radio button that is selected.
- Audience Id**: A text field containing "http://www.samplesite.com".
- Assertion Consumer Certificate**: A text area containing a long base64 encoded string:
 

```
MIIEEDjCCA3egAwIBAgICANAwDQYJKoZIhvcNAQEE
BQAwgasxCzAJBgNVBAYTA1VT
MR0wGwYDVQQIEExREaXN0cm1jdCBvZiBDb2x1bWJp
YTETMBEGA1UEBxMKV2FzaGlu
Z3RvbGJEOHCTGA1UEChMER2VudXJhbCBTZXJ2aWN1
cyBBZG1pbm1zdHJhdG1vbGJERk
```
- Assertion Consumer URL (artifact)**: A text field containing "https://www.samplesite.com/artifactreceiver".
- Create**: A button at the bottom right of the form.

**Figure 16-4: New Site Meta Data**

The administration console screen should appear providing a listing of all configured sites as shown in Figure 16-5. Next, click on the newly created site.

**Administration Console**

**Admin Tasks**

- [Download Meta Data](#)
- [Manage Sites](#)
- [New Site](#)
- [Manage User Federations](#)
- [View Server Audit Log](#)
- [Manage Admins](#)
- [New Admin](#)
- [View Admin Audit Log](#)

Logged In As: admin  
[View / Edit Profile](#)  
[Log Out](#)

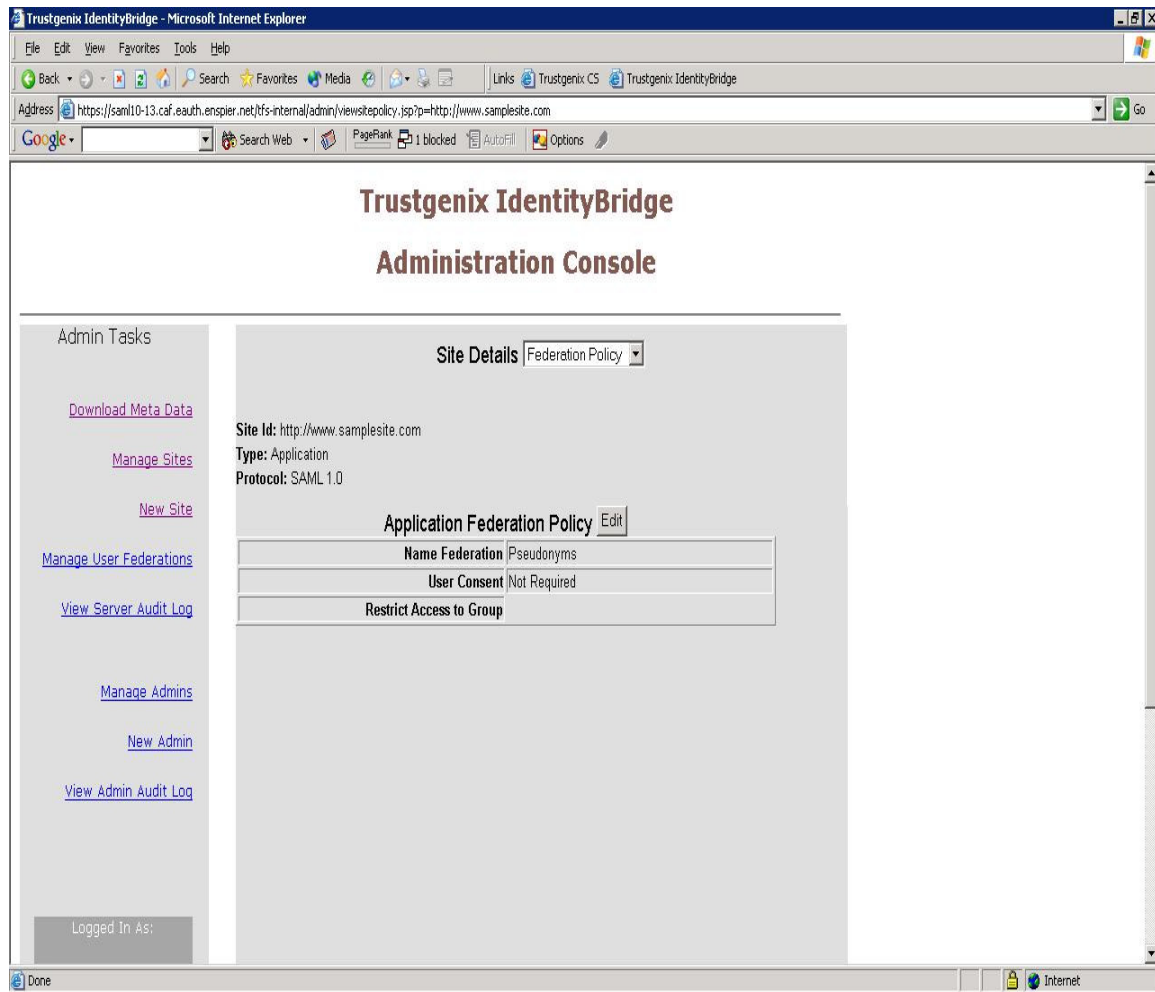
| Sites  |   |                         |                         |
|--|---|-------------------------|-------------------------|
| Name   | Id  | Type                    | Date                    |
| <input type="checkbox"/> <a href="#">IBM CS/AA</a>                               | https://08SAML10-09.caf.eauth.enspier.net | Application / Authority | 2004-11-19 09:17:13.727 |
| <input type="checkbox"/> <a href="#">Entegrity AA and CS</a>                     | http://E1-S2K3.caf.eauth.enspier.net      | Application / Authority | 2002-01-28 04:07:52.368 |
| <input type="checkbox"/> <a href="#">HP CS AA</a>                                | http://E1-S4K1.caf.eauth.enspier.net      | Application / Authority | 2004-11-17 12:37:29.54  |
| <input type="checkbox"/> <a href="#">ShareID CS AA</a>                           | https://08SAML10-10.caf.eauth.enspier.net | Application / Authority | 2004-11-17 14:12:58.323 |
| <input type="checkbox"/> <a href="#">Entrust AA CS</a>                           | http://e1-s6k2.caf.eauth.enspier.net      | Application / Authority | 2004-11-17 14:37:31.637 |
| <input type="checkbox"/> <a href="#">RSA AA CS</a>                               | _15a96784396d93deb5ee015873d0508d3a9c415c | Application / Authority | 2004-11-17 15:27:49.437 |
| <input type="checkbox"/> <a href="#">SUN CS/AA</a>                               | saml10-01.caf.eauth.enspier.net:80        | Application / Authority | 2004-11-17 15:42:42.151 |
| <input type="checkbox"/> <a href="#">Netegrity AA/CS</a>                         | http://www.netegrity.com/SiteMinder       | Application / Authority | 2004-11-19 14:36:46.703 |
| <input type="checkbox"/> <a href="#">https://saml10-10.caf.eauth.enspier.net</a> | https://SAML10-10.caf.eauth.enspier.net   | Application / Authority | 2004-12-20 14:43:25.519 |
| <input type="checkbox"/> <a href="#">Sample Site Name</a>                        | http://www.sample-site.com                | Application             | 2004-12-21 09:46:32.575 |

[Remove](#)

Done saml10-13.caf.eauth.enspier.net AdBlock

**Figure 16-5: Newly Created Site**

The Site Details screen should appear as shown in Figure 16-6. As demonstrated in Figure 16-6, select **Federation Policy** from the drop down menu and click the **Edit** button.



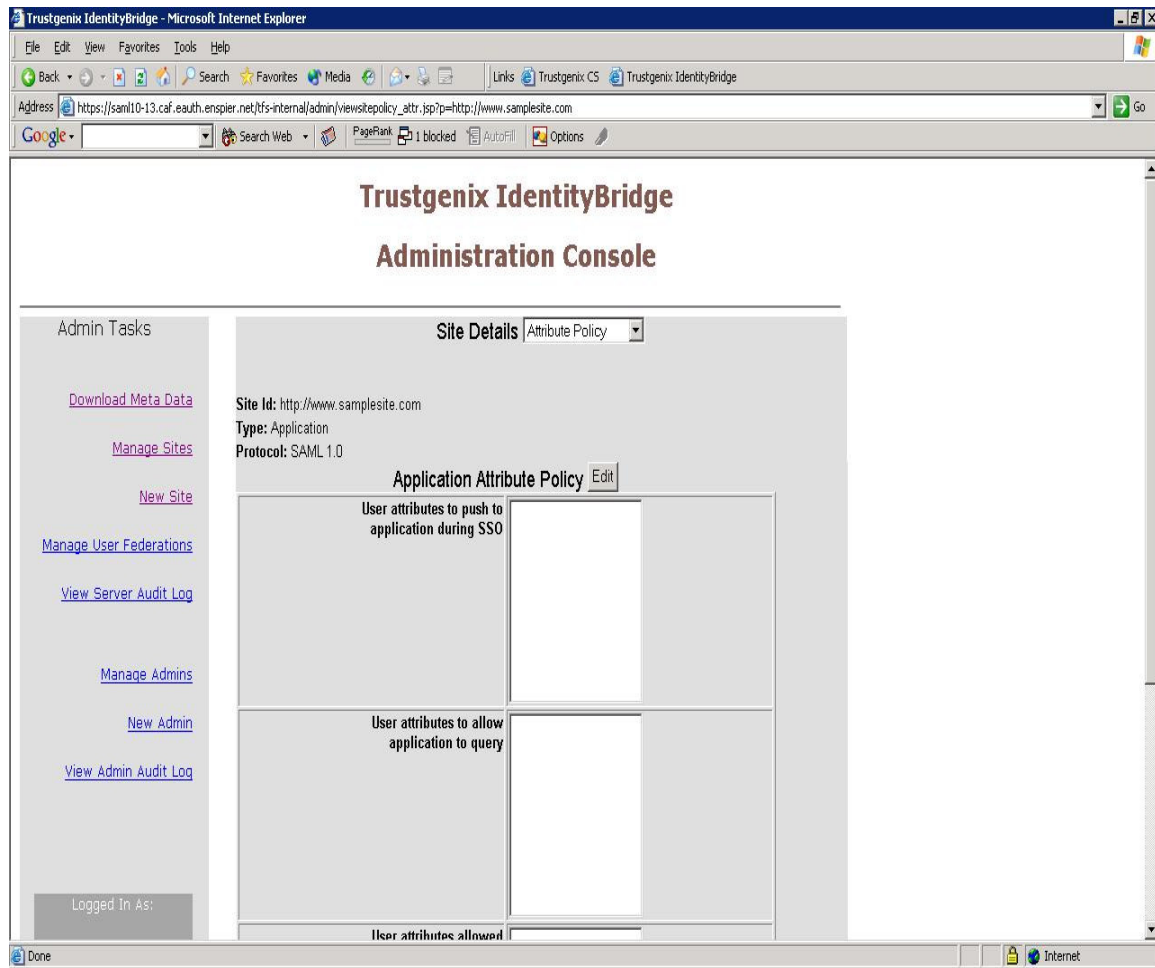
**Figure 16-6: Site Details**

The Edit Site Federation Policy screen should appear as shown in Figure 16-7. As demonstrated in Figure 16-7, select **Local Names** from the **Name Federation** drop down menu, select **Required** from the **User Consent** drop down menu, and then click the **Save** button.

The screenshot shows a Microsoft Internet Explorer browser window displaying the Trustgenix IdentityBridge Administration Console. The browser's address bar shows the URL: `https://sam10-13.caf.eauth.enspiner.net/dfs-internal/admin/editsitepolicy.jsp?p=http://www.samplestie.com`. The console has a title bar "Trustgenix IdentityBridge - Microsoft Internet Explorer" and a menu bar with "File", "Edit", "View", "Favorites", "Tools", and "Help". Below the menu bar is a toolbar with icons for Back, Forward, Stop, Home, Search, Favorites, Media, and a "Go" button. A search bar with the Google logo is also present. The main content area is titled "Trustgenix IdentityBridge Administration Console". On the left is a sidebar with "Admin Tasks" including links for "Download Meta Data", "Manage Sites", "New Site", "Manage User Federations", "View Server Audit Log", "Manage Admins", "New Admin", and "View Admin Audit Log". At the bottom of the sidebar is a "Logged In As:" box. The main content area is titled "Edit Site Federation Policy" and contains the following fields: "Site Id" with the value "http://www.samplestie.com", "Type" with the value "Application", "Name Federation" with a dropdown menu showing "Local Names", "User Consent" with a dropdown menu showing "Required", and "Restrict Access to Group" with an empty text box. At the bottom of the form are "Save" and "Cancel" buttons. The browser's status bar at the bottom shows "Done" and "Internet".

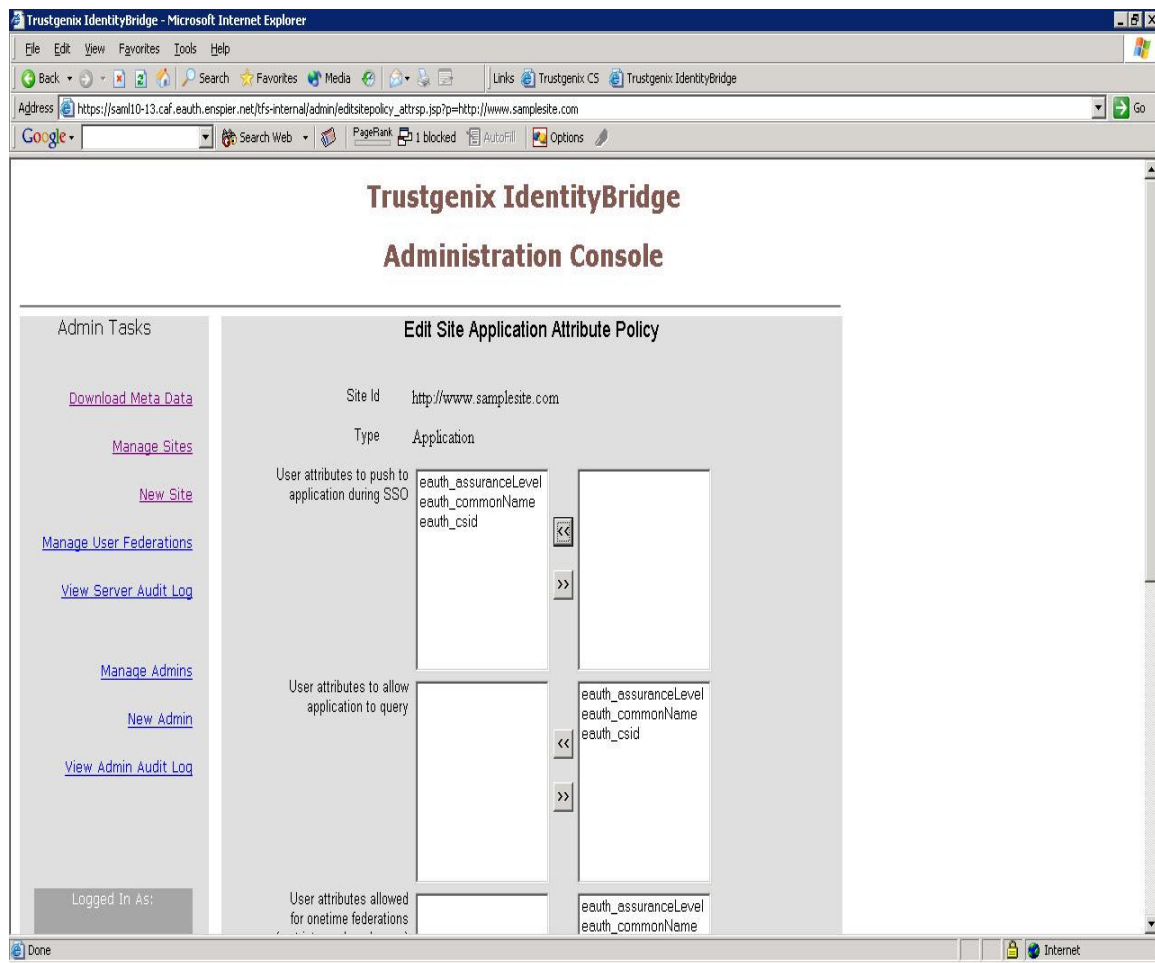
**Figure 16-7: Edit Site Federation Policy**

The Site Details and Application Attribute Policy screen should appear as shown in Figure 16-8. As demonstrated in Figure 16-8, select **Attribute Policy** from the drop down menu and click the **Edit** button.



**Figure 16-8: Site Details and Application Attribute Policy**

The Edit Site Application Attribute Policy screen should appear as shown in Figure 16-9. As demonstrated in Figure 16-9, configure **User attributes to push to application during SSO** to all desired attributes (**Assurance Level, CSid, Common Name**) and click the **Save** button.



**Figure 16-9: Edit Site Application Attribute Policy**

### 2.3 Configure a Partner CS

First, open the Trustgenix IdentityBridge Administration Console as previously described (Figure 16-1 and 16-2). As demonstrated in Figure 16-10, select **Authority** from the **Site Type** drop down menu, enter a **name** for the site in the **Site Name** field, select **SAML 1.0** from the **Protocol** drop down menu, and select the **Next** button.

The screenshot shows a web browser window titled "Trustgenix IdentityBridge - Microsoft Internet Explorer". The address bar shows the URL "https://saml10-13.caf.eauth.enspiet.net/tfs-internal/admin/newsite.jsp". The page title is "Trustgenix IdentityBridge Administration Console".

On the left side, there is a sidebar with the heading "Admin Tasks" and several links: "Download Meta Data", "Manage Sites", "New Site", "Manage User Federations", "View Server Audit Log", "Manage Admins", "New Admin", and "View Admin Audit Log". At the bottom of the sidebar, it says "Logged In As:".

The main content area is titled "New Site" and contains the following form fields:

- Site Type**: A dropdown menu with "Authority (IDP)" selected.
- Site Name**: A text input field containing "Sample Authority".
- Homepage URL**: An empty text input field.
- Description**: An empty text input field.
- Logo URL**: An empty text input field.
- Logo Text**: An empty text input field.
- Protocol**: A dropdown menu with "SAML 1.0" selected.
- Next**: A button at the bottom of the form.

Figure 16-10: Select Authority

The New Site Meta Data screen should appear as shown in Figure 16-11. As demonstrated in Figure 16-11, click on the **Manual Entry** radio button, enter the site's **Issuer ID** in the **Issuer ID** field, enter the site's **hex Source ID** in the **Source ID** field (*note: cannot be Base64 encoded*), enter the **responder URL** in the **Artifact Retrieval SOAP Endpoint** field, and then click the **Create** button.

The screenshot shows a web browser window titled "Trustgenix IdentityBridge - Microsoft Internet Explorer". The address bar shows the URL "https://saml10-13.caf.eauth.enspiet.net/tfs-internal/admin/upload.jsp". The page content is titled "Trustgenix IdentityBridge Administration Console". On the left, there is a sidebar with "Admin Tasks" including links for "Download Meta Data", "Manage Sites", "New Site", "Manage User Federations", "View Server Audit Log", "Manage Admins", "New Admin", and "View Admin Audit Log". The main content area is titled "New Site Meta Data" and contains a form with the following fields and values:

- Type: Authority
- Protocol: SAML 1.0
- Meta Data File: (empty) [Browse...]
- Meta Data URL: (empty)
- Manual Entry: (selected)
- Issuer Id: https://www.sampleauthority.com
- Source ID: d7c363ec97c5f9bee8b0defcd232fbd1306c36
- Artifact Retrieval SOAP Endpoint: https://www.sampleauthority.com:7676/respc
- Attribute Authority SOAP Endpoint: (empty)
- Intersite Transfer URL: (empty)
- [Create]

At the bottom left, it says "Logged In As:".

**Figure 16-11: New Site Meta Data**

The administration console screen should appear providing a listing of all configured sites as shown in Figure 16-12. Next, click on the newly created site.

The screenshot shows the Trustgenix IdentityBridge Administration Console in a Mozilla Firefox browser window. The URL is <https://saml10-13.caf.eauth.enspier.net/tfs-internal/admin/index.jsp>. The page title is "Trustgenix IdentityBridge Administration Console".

On the left, there is a sidebar with "Admin Tasks" including links for "Download Meta Data", "Manage Sites", "New Site", "Manage User Federations", "View Server Audit Log", "Manage Admins", "New Admin", and "View Admin Audit Log". At the bottom of the sidebar, it shows "Logged In As: admin" and a "View / Edit Profile" link.

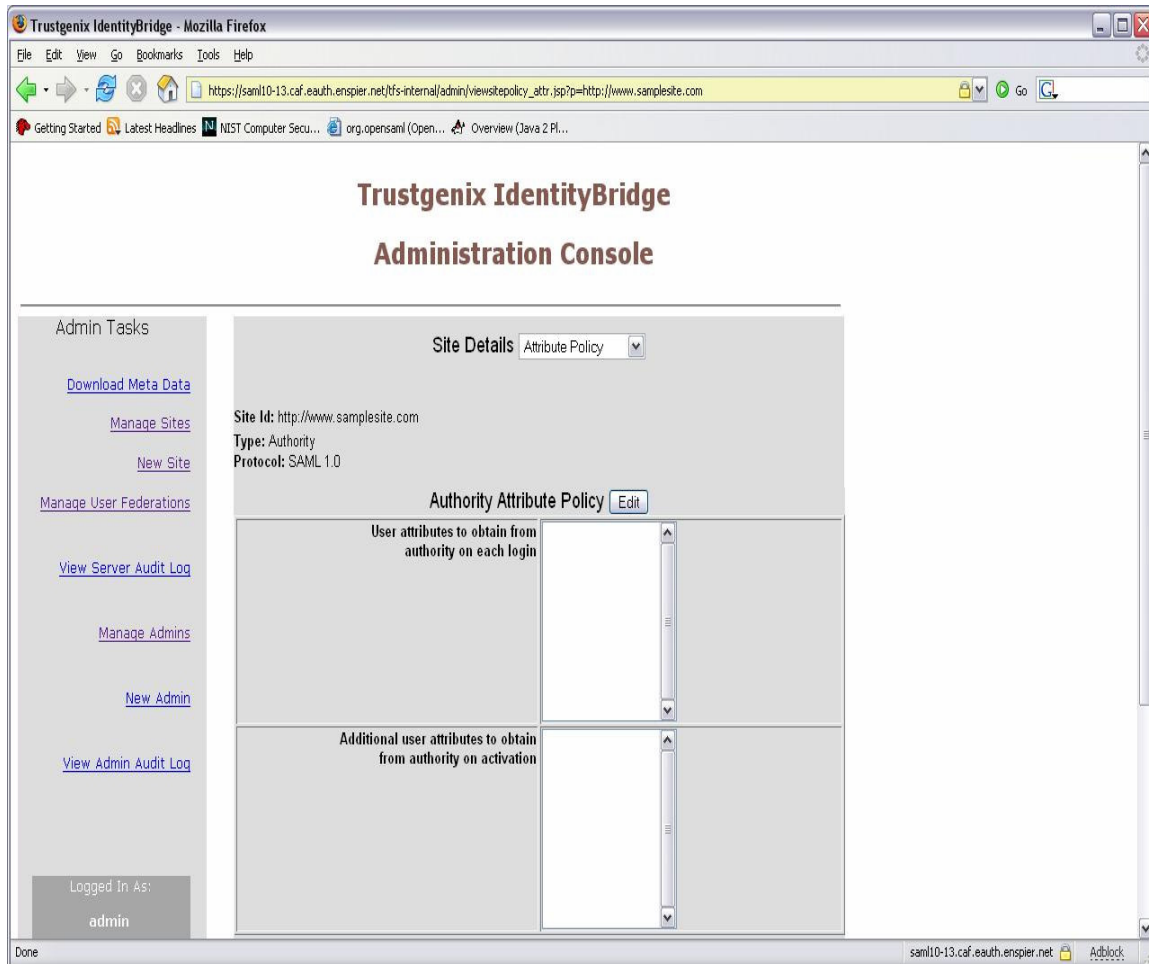
The main content area is titled "Sites" and contains a table with the following columns: Name, Id, Type, and Date. The table lists several configured sites, including "IBM CS/AA", "Entegry AA and CS", "HP CS AA", "ShareID CS AA", "Entrust AA CS", "RSA AA CS", "SUN CS/AA", "Netegrity AA/CS", "https://saml10-10.caf.eauth.enspier.net", and "Sample Authority". Each site entry has a checkbox to its left.

| Name  | Id  | Type                    | Date                    |
|---|---|-------------------------|-------------------------|
| <a href="#">IBM CS/AA</a>                               | <a href="https://08SAML10-09.caf.eauth.enspier.net">https://08SAML10-09.caf.eauth.enspier.net</a>               | Application / Authority | 2004-11-19 09:17:13.727 |
| <a href="#">Entegry AA and CS</a>                       | <a href="http://E1-S2K3.caf.eauth.enspier.net">http://E1-S2K3.caf.eauth.enspier.net</a>                         | Application / Authority | 2002-01-28 04:07:52.368 |
| <a href="#">HP CS AA</a>                                | <a href="http://E1-S4K1.caf.eauth.enspier.net">http://E1-S4K1.caf.eauth.enspier.net</a>                         | Application / Authority | 2004-11-17 12:37:29.54  |
| <a href="#">ShareID CS AA</a>                           | <a href="https://08SAML10-10.caf.eauth.enspier.net">https://08SAML10-10.caf.eauth.enspier.net</a>               | Application / Authority | 2004-11-17 14:12:58.323 |
| <a href="#">Entrust AA CS</a>                           | <a href="http://e1-s6k2.caf.eauth.enspier.net">http://e1-s6k2.caf.eauth.enspier.net</a>                         | Application / Authority | 2004-11-17 14:37:31.637 |
| <a href="#">RSA AA CS</a>                               | <a href="https://15a96784396d93deb5ee015873d0508d3a9c415c">https://15a96784396d93deb5ee015873d0508d3a9c415c</a> | Application / Authority | 2004-11-17 15:27:49.437 |
| <a href="#">SUN CS/AA</a>                               | <a href="https://saml10-01.caf.eauth.enspier.net">https://saml10-01.caf.eauth.enspier.net</a>                   | Application / Authority | 2004-11-17 15:42:42.151 |
| <a href="#">Netegrity AA/CS</a>                         | <a href="http://www.netegrity.com/SiteMinder">http://www.netegrity.com/SiteMinder</a>                           | Application / Authority | 2004-11-19 14:36:46.703 |
| <a href="#">https://saml10-10.caf.eauth.enspier.net</a> | <a href="https://SAML10-10.caf.eauth.enspier.net">https://SAML10-10.caf.eauth.enspier.net</a>                   | Application / Authority | 2004-12-20 14:43:25.519 |
| <a href="#">Sample Authority</a>                        | <a href="http://www.sample-site.com">http://www.sample-site.com</a>   | Authority               | 2004-12-21 09:49:00.117 |

At the bottom of the table, there is a "Remove" button. The browser status bar at the bottom shows "Done" and the address "saml10-13.caf.eauth.enspier.net".

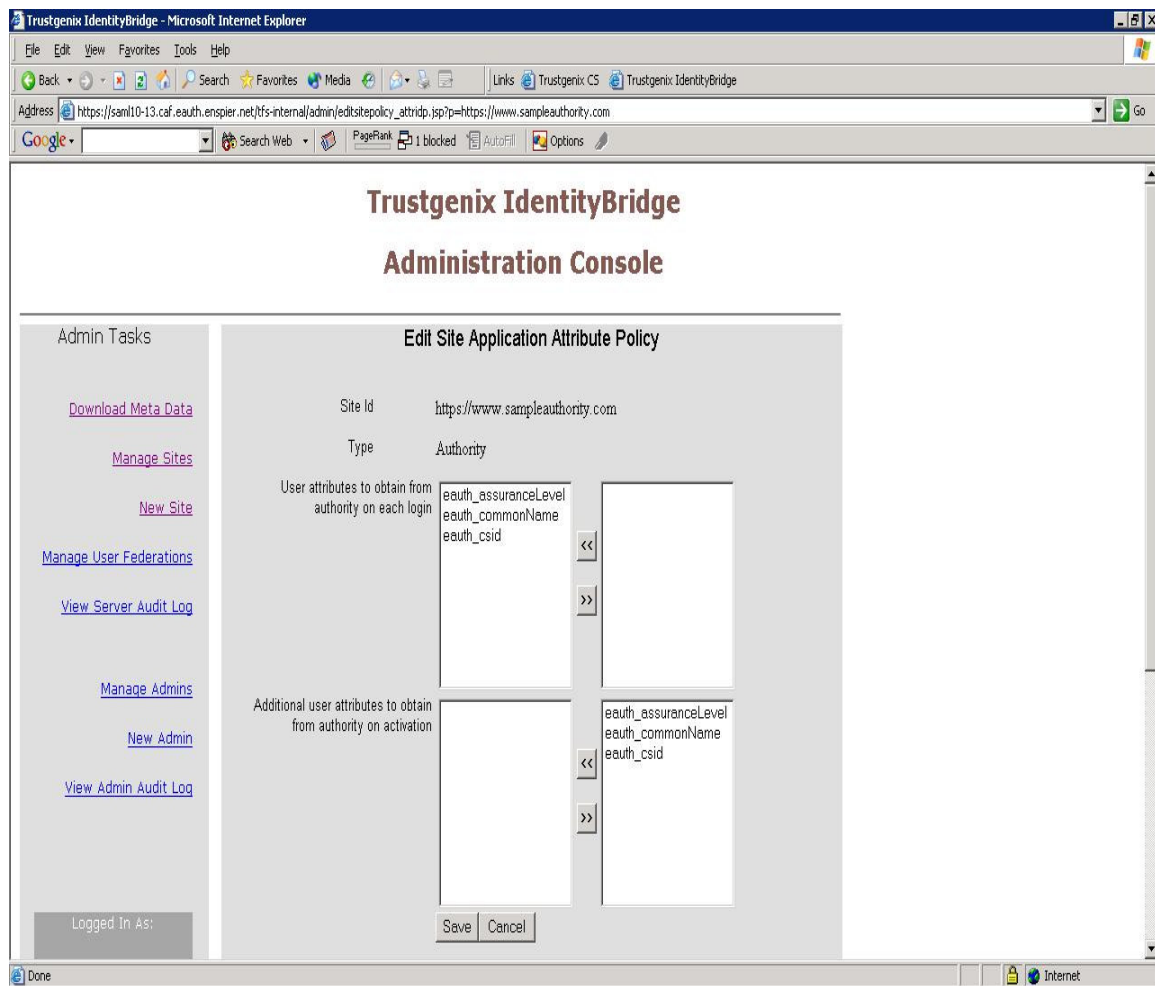
**Figure 16-12: Newly Created Site**

The Site Details and Attribute Policy screen should appear as shown in Figure 16-13. As demonstrated in Figure 16-13, select **Attribute Policy** from the drop down menu and click the **Edit** button.



**Figure 16-13: Site Details and Attribute Policy**

The Edit Site Application Attribute Policy screen should appear as shown in Figure 16-14. As demonstrated in Figure 16-14, configure **User attributes to obtain from authority on each login** to all desired attributes (**Assurance Level, CSid, Common Name**) and click the **Save** button.



**Figure 16-14: Edit Site Application Attribute Policy**